WHAT IS CLAIMED IS:

1. A system for securing an application for execution on a computer, the method comprising:

a preprocessor module for scanning the application program for code sequences that cause the computer to trap to the operating system and for modifying the code sequences such that the computer does not trap to the operating system;

a server computer for receiving at least one application that has been modified by the preprocessor module;

a network; and

a client computer operably connected to the server computer via the network, wherein the client computer receives the modified application from the server computer, wherein subsequent to receiving the application, the client computer executes the application.

2. A method of securing an application for execution on a computer, the method comprising:

scanning the application for code sequences that cause the computer to trap to the operating system; and

modifying the code sequences such that the computer does not trap to the operating system.

3. A method of securing an application for execution on a computer, the method comprising:

loading the application;

marking all of the code pages of the loaded application execute only; and

preventing the application from creating executable data during the execution of the application.

09725305.112500

4. A method of securing an application for execution on a computer, the method comprising:

preventing the application from creating executable data during the execution of the application;

scanning the application for code sequences that cause the computer to trap to the operating system; and

modifying the code sequences such that the computer does not trap to the operating system.

5. A method of securing an application for execution on a computer, the method comprising:

preventing the application from creating executable data during the execution of the application; and

preventing at least one code page of the application from becoming readable and writeable.

6. A method of securing an application for execution on a computer, the method comprising:

loading the application;

marking all of the data pages of the loaded application read and write only; and

preventing the application from creating executable data during the execution of the application.

7. A method of securing an application for execution on a computer, the method comprising:

preventing the application from creating executable data during the execution of the application; and

preventing the application from modifying executable files or executing any application generated files.

8. The method of Claim 7, additionally comprising:

scanning the application for code sequences that cause the computer to trap to the operating system; and

modifying the code sequences such that the computer does not trap to the operating system.

9. The method of Claim 7, additionally comprising preventing at least one code page of the application from becoming readable and writeable.

10. The method of Claim 7, additionally comprising:

loading the application; and

marking all of the code pages of the loaded application execute only.

11. The method of Claim 7, additionally comprising:

loading the application; and

marking all of the data pages of the loaded application read and write only.

12. The method of Claim 7, wherein preventing the code page of the application from becoming readable and writeable comprises intercepting transparently to the application a request from the application to change the attributes of the code page.

13. A method of securing an application for execution on a computer, the method comprising:

before the execution of an application program, scanning the application program for code sequences that cause the computer to trap to the operating system;

before the execution of the application program, modifying the code sequences such that the computer does not trap to the operating system;

09727305.112900

during or subsequent to the execution of the application program, scanning executable data that is created by the application program for sequences that trap to the operating system; and

during or subsequent to the execution of the application program, scanning new executable files that are created or modified by the application program; and

during or subsequent to the execution of the application program, modifying the executable data and the new files such that the application program does not trap to the operating system.

14. A method of securing an application for execution on a computer, the method comprising:

scanning the application for code sequences that cause the computer to trap to the operating system;

modifying the code sequences such that the computer does not trap to the operating system;

scanning the dynamically generated code that is created by the application for code sequences that cause the computer to trap to the operating system; and

modifying the code sequences such that the computer does not trap to the operating system.

15. The method of Claim 14, additionally comprising preventing at least one code page of the application from becoming readable and writeable.

16. The method of Claim 15, wherein preventing the code page of the application from becoming readable and writeable comprises intercepting transparently to the application a request from the application to change the attributes of the code page.

09723305.112600

17. The method of Claim 14, additionally comprising preventing data pages from becoming executable.

18. A system for preventing an application from directly calling an operating system, the system comprising:

means for scanning the application program for code sequences that cause the computer to trap to the operating system; and

means for modifying the code sequences such that the computer does not trap to the operating system.

19. A system for preventing an application from directly calling an operating system, the system comprising:

means for preventing the application from creating executable data during the execution of the application; and

means for preventing the application from modifying executable files or executing any application generated files.

20. The system of Claim 19, additionally comprising:

means for scanning the application program for code sequences that cause the computer to trap to the operating system; and

means for modifying the code sequences such that the computer does not trap to the operating system.

21. The system of Claim 19, additionally comprising means for copying the location of at least one module from a first location to a second location.

22. The system of Claim 19, wherein the at least one module is a system library.

23. The system of Claim 19, additionally comprising means for preventing at least one code page of the application from becoming readable and writeable.

09723205.112600

24. The method of Claim 19, wherein preventing the code page of the application from becoming readable and writeable comprises intercepting transparently to the application a request from the application to change the attributes of the code page.

25. A system for securing an application for execution on a client computer, the system comprising:

means for scanning the application for code sequences that cause the computer to trap to the operating system;

means for modifying the code sequences such that the computer does not trap to the operating system;

means for scanning the dynamically generated code, that is created by the application, for code sequences that cause the computer to trap to the operating system; and

means for modifying the code sequences such that the computer does not trap to the operating system.

09727305.112500

26. The system of Claim 25, additionally comprising means for copying the location of at least one module from a first location to a second location.

27. The system of Claim 25, wherein the at least one module is a system library.

28. The system of Claim 25, additionally comprising means for preventing at least one code page of the application from becoming readable and writeable.

29. The system of Claim 25, wherein preventing the code page of the application from becoming readable and writeable comprises intercepting transparently to the application a request from the application to change the attributes of the code page.